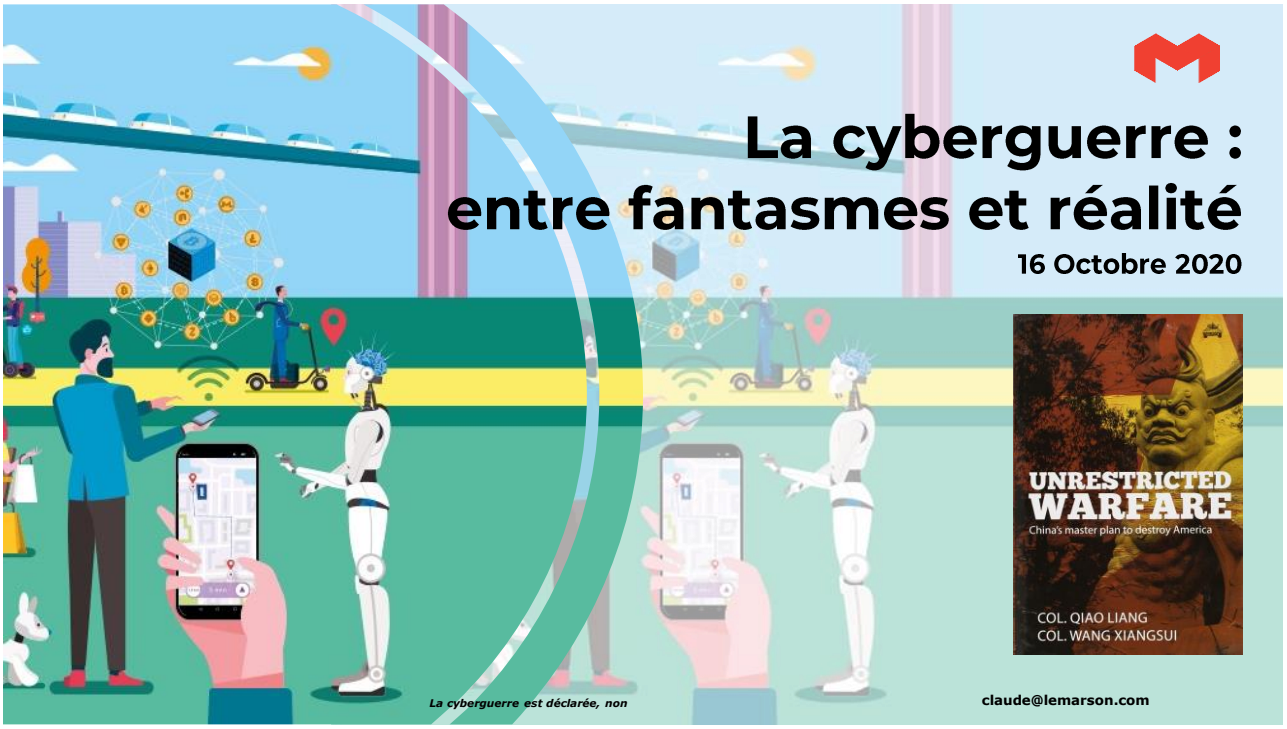
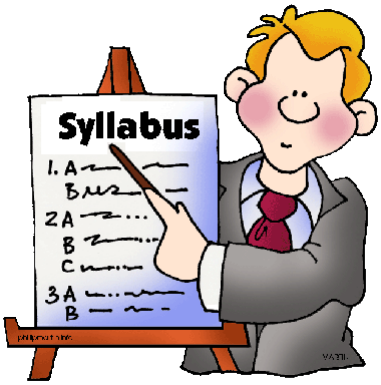


Entre 2009 et 2018, augmentation de 440 % des attaques liées à un objectif politique

Sommaire

La cyberguerre : entre fantasmes et réalité



Une cyber attaque gouvernementale ("cyber warfare") est une attaque menée par un état ou une structure opérationnelle pour le compte d'un état, par des moyens numériques conventionnels ou innovants, avec pour objectif de détruire ou d'empêcher le fonctionnement d'installations vitales, de récupérer des informations confidentielles, de déstabiliser une cible politique, etc

Globalement la cyberguerre ou présumée telle…

Ca, c'est ce que l'on dit

L'hypocrisie à hauteur d'une institution

- En 2016, la Corée du Nord a attaqué la Corée du Sud, une prestation qui a duré 1 an et permis aux « troupes » de Kim Jong-Un de voler 42 000 documents confidentiels, dont 95 % liés à la défense (140 000 machines gouvernementales ont été ciblées).
- La Russie avait procédé à des attaques du même type contre l'Estonie puis durant son conflit en 2008 avec la Géorgie et enfin, plus récemment contre l'Ukraine.
- Quant aux chinois, un rapport datant de 2013 dû à Joe McReynolds, expert en stratégie militaire du Centre américain de recherche et d'analyse sur le renseignement, indique qu'ils disposent d'unités de pirates informatiques avec 3 catégories d'intervenants : des militaires, des civils y compris dans les organisations gouvernementales et des groupes indépendants, qui peuvent être mobilisés, si le besoin s'en fait sentir.
- Les Etats-Unis font la même chose, tout comme les européens.
- Nous assisterons peut-être à la première attaque, revendiquée comme telle, d'un pays contre un autre. Ouvertement et sans états d'âmes. Nous franchirons un palier supplémentaire, la conjoncture au Moyen-Orient, aux Etats-Unis et en Europe, s'y prêtant à merveille.

La cyberguerre est un fantasme

Mais on peut contester…

- La guerre se définit comme un état de conflit armé entre des groupes politiques constitués, tels que des États
- Définition qui ne s'applique pas à la cyberguerre ou guerre électronique
- On confond l'outil avec la finalité
- Même confusion que guerre bactériologique
- On confond l'acte de malveillance politique, qui peut déstabiliser un pays, avec une véritable guerre
- C'est un fantasme journalistique destiné à frapper les imaginations
- Il s'agit de l'usage de moyens électroniques, classiques en sécurité, destinés à accompagner des opérations ciblées à vocation politique, militaire ou économique
- La Russie n'a pas déclaré la guerre aux Etats-Unis, ni à la Corée du Sud
- Le Canada n'a pas envoyé ses ambassadeurs à la Chine…
- Il faut parler de **cyber déstabilisation**, de **cyber désinformation**, de **cyber destruction**, etc, qui peuvent avoir des conséquences graves dans la vie politique (élections US de 2016), mais pas de guerre au sens étymologique du mot
- Dans les faits, ce sont des actions numériques isolées ou synchronisées, à caractère politique ou militaire, qui ont les mêmes conséquences qu'une agression classique, menées par des états
- On a simplement changé de terrain de jeu et on emploie des moyens nouveaux
- Ce qui n'enlève rien à la dangerosité des actes et à l'opposition classiques des blocs est-ouest

Pourquoi sommes-nous aussi vulnérables

- Dépendance croissante à l'informatique
  - Demain tout sera piloté par logiciel
  - De nombreuses activités manuelles auront été remplacées par des robots, de même que certains services fondamentaux : hôpitaux, défense, banques…
  - Les services "régaliens" d'état sont souvent connectés (hors armée) aux réseaux traditionnels, sans rupture : production d'eau, production d'énergie, recherche fondamentale, espace…
  - Les véhicules vont devenir autonomes : voitures, camions, bateaux, avions, trains
- Eternel problème de la faiblesse des infrastructures Internet
- Anonymat des opérations : TOR, DOH
- Connectique de partout : satellites basse altitude, cellulaires, la connexion n'est plus un problème
- Les objets connectés vont tout envahir : 4 ème génération des systèmes d'information
  - L'univers domestique sera "objetisé", avec deux conséquences, l'accès aux données personnelles et une connectique faiblement protégée
  - Les usines seront fondées sur des capteurs : sécurité, gestion, mais surtout production
- Demain, la dépendance sera totale par rapport aux réseaux : 5G, 6G, connectique professionnelles et personnelle
- La motivation des troupes d' "en face" ne doit pas être sous-estimée
- Leur volonté de revanche
- Ni leur compétence, qui est grande
  - La Russie, les ex pays de l'est et la Chine, ont une longue tradition d'excellence en mathématiques et en éducation scientifique
  - Ils sont parfaitement autonomes et peuvent produire les techniques les plus sophistiquées d'attaques, les algorithmes de chiffrement les plus impénétrables…
- Mondialisation, tout est accessible

Surtout ne pas sous-estimer la compétence et la motivation de "ceux d'en face"…

Ce que n'est pas une cyber structure étatique d'attaque

- Ne pas confondre organisations gouvernementales avec groupes mafieux
- Bien que certains états entretiennent des relations suivies avec eux
- Ce ne sont pas des armées, mais des groupes technologiques, dépendants de structures en place, qui apportent leur contribution aux conflits
- L'exemple du groupe de renseignement russe Sandworm, l'un des pires de l'histoire
  - En 2014 : attaque du réseau électrique ukrainien : verrouillage des installations, alimentation de secours des salles de contrôle coupée : 250 000 ukrainiens ont été privés d'électricité
  - En 2016, nouvelle tentative sur l'Ukraine, avortée pour un problème de configuration
  - Juin 2017 : attaque NotPetya de grande envergure : 300 entreprises ukrainiennes hors d'état de fonctionner, la quasi-totalité des agences gouvernementales, 10 % du parc informatique ukrainien touché et irrécupérable, qui s'est répandue dans le reste du monde (Maersk, géant de la logistique, Saint-Gobain)
  - Coût estimé de NotPetya : 10 milliards $
  - 2017 : Sandworm cible les JO de PyeongChang (Corée du Sud)

Des milliers de machines bloquées par NotPetya

C'est quoi une cyberpuissance ?

- Plus de 30 pays ont développé des capacités d'attaques
- Le NCPI (National Cyber Power Index) définit les 7 objectifs d'une cyberpuissance (centre Belfer de Harvard) :
  - Surveiller et contrôler les groupes nationaux et forces de persuasion
  - Renforcer et améliorer les cyberdéfenses nationales
  - Contrôler et manipuler l'information
  - Collecter des renseignements à l'étranger pour la sécurité nationale
  - Accroître les compétences nationales en matière de technologies applicables à la cybersécurité
  - Détruire ou désactiver l'infrastructure et les capacité de l'adversaire
  - Définir les normes internationales en cybersécurité
- NCPI définit 32 indicateurs d'intention et 27 indicateurs de capacité

#	Surveillance	Defense	Information Control	Intelligence	Commercial	Offense	Norms
1	US	China	US	US	US	Russia	US
2	UK	Singapore	Russia	UK	South Korea	US	France
3	France	Canada	China	China	China	China	Japan
4	China	France	South Korea	Germany	Japan	Germany	China
5	Japan	Switzerland	Sweden	Singapore	UK	UK	Germany
6	Sweden	Netherlands	Singapore	Israel	Singapore	France	Singapore
7	Canada	US	UK	France	Netherlands	Netherlands	UK
8	Germany	Japan	New Zealand	Malaysia	Germany	Spain	Malaysia
9	New Zealand	Germany	Saudi Arabia	Estonia	France	Estonia	South Korea
10	Israel	Sweden	Canada	Netherlands	Switzerland	Canada	India

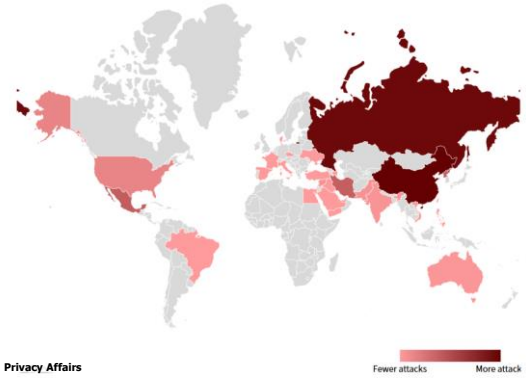
Belfer Center
National Cyber Power Index 2020 "Top 10"

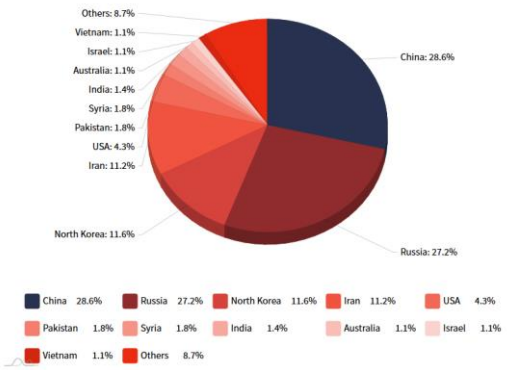
#	Country	Overall score	Specific Rankings: Capability	Specific Rankings: Intent
1	**United States**	50.24	1	2
2	**China**	41.47	2	1
3	**United Kingdom**	35.57	3	3
4	**Russia**	28.38	10	4
5	**Netherlands**	24.18	9	5
6	**France**	23.43	5	11
7	**Germany**	22.42	4	12
8	**Canada**	21.50	11	9
9	**Japan**	21.03	8	14
10	**Australia**	20.04	16	8

Les statistiques (...)
La période angélique est terminée

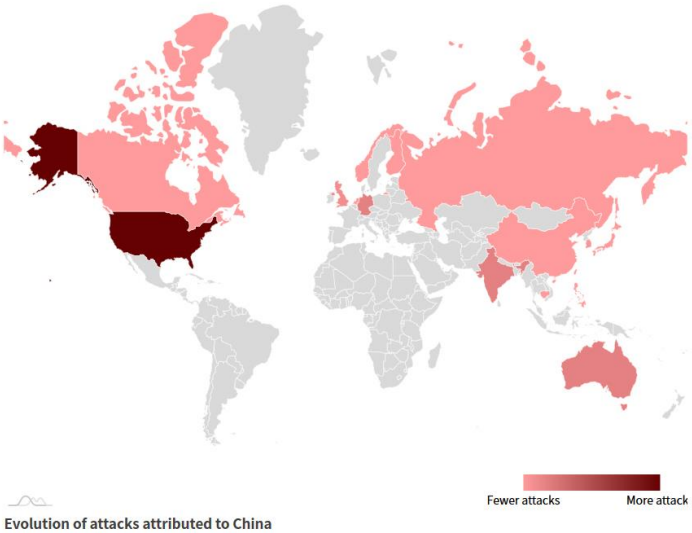
- Il faut s'en méfier : tout dépend des sources
- On a peu d'informations sur les organisations russes et chinoises, autrement que par des agences américaines…
- Le budget US en 2020 est de 17 milliards $, sans doute beaucoup plus…
- Entre 2009 et 2018 : 440 % d'augmentation des cyber attaques
- 26,3 % des attaques sont dirigées contre les USA
- 32 % des attaques chinoises visaient les USA entre 2009 et 2018, mais aussi Hong Kong (6,3 %), l'Australie (6,3 %), l'Allemagne (6 %), l'Europe (3,8 %) et le Royaume Uni (3,6 %)
- 35 % des attaques sont politiquement motivées par des liens avec la Chine ou la Russie
- 11 % des attaques sont en relation avec l'espionnage
- Ceci à replacer dans le contexte global de la cybersécurité, qui n'est pas que gouvernementale
  - En 2017, le Gouvernement fédéral US a relevé plus de 35 200 incidents de cyber sécurité, ayant un lien potentiel avec des organisations étrangères

D'où viennent les cyberattaques





La cible des cyberattaques chinoises



Evolution of attacks attributed to China

L'organisation russe

L'organisation chinoise

"Specialized military network warfare forces". Des unités opérationnelles spécialisées dans l'attaque des réseaux et leur défense.

"PLA Authorized Forces", spécialistes de la warfare, créé en 2015. Dépend de deux ministères : MSS ("Ministry of State Security", la CIA chinoise et le MPS ("Ministry of Public Security".

Forces non gouvernementales, civils et militaires qui collaborent.

- L'information et la désinformation sont très actives concernant la Chine
- Canada
  - L'activité de plusieurs départements du gouvernement fédéral est compromise en 2011
  - En 2014 : des hackers chinois attaquent les machines du "National Research Council"
- USA
  - 2010 : Google indique une attaque de ses structures "corporate", mais aussi 34 autres compagnies
  - 2014 : Implication chinoise dans le vol d'informations confidentielles de compagnies privées US
  - 2014 : Des hackers associés au gouvernement chinois entrent dans les systèmes de compagnies aériennes US et d'entreprises impliquées dans le suivi et coordination des mouvements de troupes US
  - 2019 : Attaques sur la US Navy et certains de ses partenaires
  - 2020 : Un grand jury US établit que 4 membres de l'armée de libération populaire sont impliqués dans l'attaque Equifax de 2017

La part de vérité est difficile à établir : tout dépend du côté où l'on se place

L'organisation US

US Army
Branche de l'armée de l'US Cyber Command
Constituée de :
9th Army Signal Command (Army Network Enterprise echnology Command"), une partie de la "1st Information Operations Command" et United States Army Intelligence and Security Command

US Marine
United States Marine Corp Forces Cyberspace Command (fait partie de l' "United States Marine Corps").

US Navy
La Fleet Cyber Forces constituée de quatre composantes :
Naval Network Warfare Command
Navy Cyber Defense Operations Command
Combined Task Forces

Air Force
La 16AF ("Sixteenth Air Force") est subdivisée en 3 composantes :
67th Network Warfare Wing
688th Information Operation Wing
689th Combat Communication Wing

Les outils

- Les cyber attaques gouvernementales se fondent sur plusieurs natures d'outils
- Les outils classiques du monde du hacking
  - Phishing
  - DDoS (Estonie)
  - Zero day Virus, chevaux de Troie et Backdoors (attaque Shamoon qui a effacé 30 000 PC de l'Aramco saoudienne)
  - Ransomware, courriels frauduleux, stéganographie
  - Attaques par force brute
  - Botnets (ex de Grum, 6 serveurs en Ukraine et un en Russie, 18 milliards de spams par jour
  - APT ("Advanced Persistent Threats")
- Les outils inconnus
  - Algorithmes de chiffrement sur des bases mathématiques nouvelles
  - Algorithmes de compréhension de cibles spécifiques
- Intelligence Artificielle
  - Machine Learning pour apprendre du comportement des cibles
  - Deep Learning pour "sortir" de masses importantes de données, des éléments structurants : état d'esprit, idées partagées…
- Outils de simulation et jumeaux numériques
- Deep fakes vidéos
- Puissance de calcul considérable
  - Machines scientifiques en clusters (les chinois sont tout en haut des palmarès, processeurs chinois et plus Intel)
  - Machines quantiques
- Seuls quelques pays ont les moyens nécessaires pour maîtriser ces ressources : Chine, Europe, OTAN, Japon, USA : syndrome de l'arme nucléaire

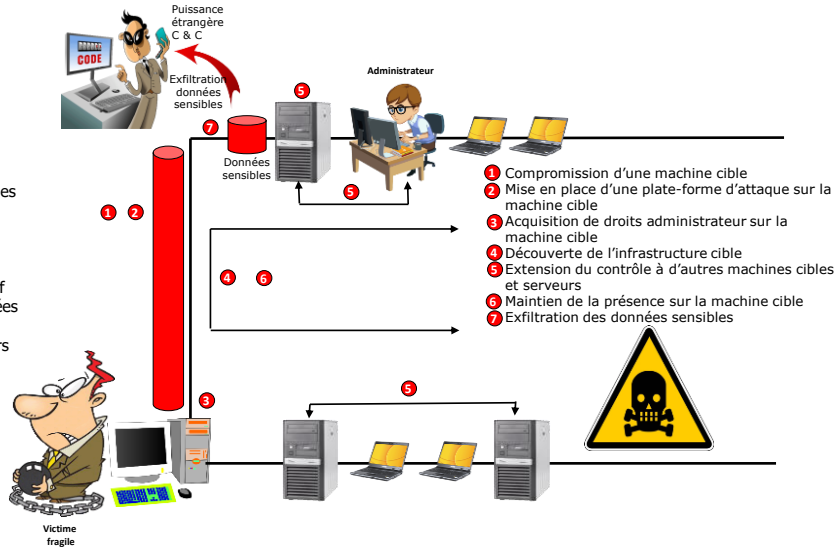
- L'opération Aurora est l'une APT les plus connue.
- Wikileaks a montré ses origines chinoises.
- L'attaque ciblait 34 structures américaines : Adobe, Juniper, Rackspace, Yahoo, Symantec, Northrop Gruman, Dow Chemical
- La perte d'informations a été considérable
- L'attaque a duré plus d'un an

La mécanique d'une attaque APT

Le maillon faible de l'être humain

L'APT est un enchaînement d'attaques par des moyens divers, en vue d'effectuer une opération délictueuse :

- **Advanced** : les techniques les plus sophistiquées sont utilisées
- **Persistent** : il y a une cible et un objectif bien précis, l'attaque peut durer des années
- **Threat** : les opérations structurées et coordonnées sont menées par des hackers compétents

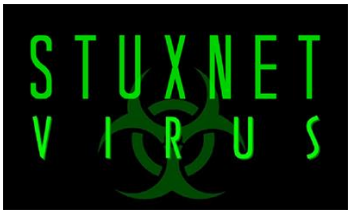


Comment se déroule une cyber attaque gouvernementale

- Exactement la même chronologie que pour une attaque classique :
  - Détermination et compréhension de la cible : pays, groupe de pression
  - Mise en place des ressources nécessaires : machines, réseaux, personnels
  - Détermination des failles existantes dans l'infrastructure "ennemie"
  - Constitution d'une APT : combinaison d'attaques, un ensemble persistant opérations, qui peut durer plusieurs années, la difficulté pour l'assailli étant de comprendre les liens entre elles
  - Lancement de l'APT et suivi opérationnel
  - Comptes-rendus d'opérations au niveau commandement
  - Adaptations aux événements et modification de l'APT

Attaques contre les structures industrielles

- Les menaces contre les structures industrielles peuvent aussi être une forme de chantage
- Le malware Triton a été conçu pour bloquer les usines an moyen-orient
  - Il communique avec certains systèmes de contrôle industriel, les SIS ("Safety Instrumented Systems") de Tricomex, dont il modifie les comportements
- En 2020, deux attaques ont visé des installations de fourniture d'eau en Israël, mais ont été détectées et stoppées : modification des niveaux de chlore dans l'eau qui aurait pu empoisonner la population locale (Galilée et province centrale de Mateh Yehuda)
  - Attaque en lien avec l'Iran (Washington Post)
  - Réplique israélienne avec une attaque du port de Shahid Rajael de la ville de Bandar Abbas en Iran
- Stuxnet est un vers conçu en 2010 par les USA et Israël (jamais confirmé), qui a coûté plusieurs millions $, qui visaient à endommager les centrifugeuses atomiques Siemens du programme nucléaire iranien (1 000 centrifugeuses ont été atteintes)
  - Le vers Stuxnet a été construit sur 4 exploits "zero day" et a donné lieu à de nombreux stuxnet-like, partout dans le monde



Le vrai problème : la désinformation

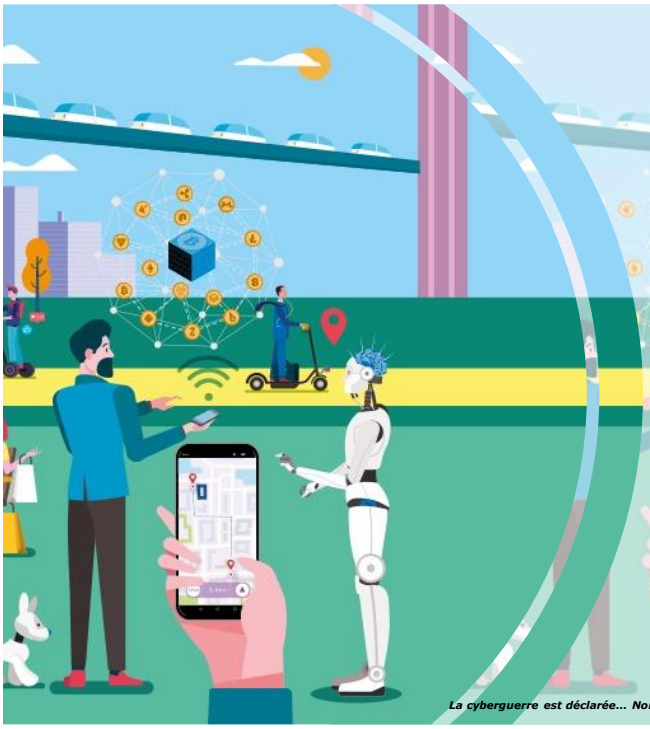
- Le vrai terrain de chasse des attaques gouvernementales est celui de l'information et de la désinformation
- L'information est la matière la plus malléable qui soit, il est facile de la modifier et de l'orienter
- On est dans la même situation que pendant la guerre froide, avec des moyens démultipliés
- Les principaux pays ont intégré des cellules de vol d'informations : il ne faut pas être hypocrite, Canada, Etats-Unis, France… c'est le "jeu"
- Les réseaux sociaux, adossés à des mécanismes d'analyse big data et à l'IA constituent une arme de "dissuasion massive", qui elle est bien réelle…
- Les agences russes ont lourdement investi les réseaux sociaux à des fins de manipulation politique
  - Ex en 2016, les GRU et FSB sont entrés dans les machines du Comité national Démocrate et ont publié des faux discours de déstabilisation concernant Hilary Clinton, révélant (juste avant la convention de juillet 2016) ses liens (ou supposés tels) avec Wall Street
  - Difficile de mesurer l'impact : mais Hilary Clinton n'a pas été élue
- La manipulation des consciences sera l'une des clés des 20 années à venir, l'IA va donner aux états des moyens nouveaux pour y parvenir
- Il sera impossible de discerner le vrai du faux, le réel du simulé

En 1917, Mata Hari était fusillée à Vincennes pour espionnage, les hackers sont les mêmes personnages, 100 ans plus tard, qui volent et diffusent des informations fausses
La différence étant que les conflits sont devenus planétaires et non plus limités à deux belligérants

Attaques gouvernementales : le "catalogue"

Que va-t-il se passer ?

- La situation actuelle va s'aggraver, mais pas au point de devenir LA guerre moderne
- Y a-t-il des solutions pour l'empêcher ? Les missiles ne s'arrêtent pas aux frontières, pas plus que les malwares…
- Les grands pays vont prolonger leur affrontement, le numérique prenant de plus en plus de place, à côté de méthodes plus traditionnelles
- Les attaques seront généralement hébergées dans le Cloud : CWaaS :Cyber Warfare as a Service
- Les sites de production à vocation terroriste continueront de s'étendre avec tous les outils nécessaires, des formations, de l'assistance
- Les attaques vont gagner en maturité, plus sophistiquées, avec de nouveaux intervenants très motivés et compétents : mouvance islamique, Pakistan, Corée du Nord, Iran, Inde…
- Tous les conflits de la planète auront une composante numérique
- Il y aura de graves attaques contre les centres vitaux, très spectaculaires, mais les "victimes" vont mieux se protéger en compartimentant leurs installations
- Le vrai souci sera la manipulation de l'information, qui va s'étendre et se diversifier : aucun mécanisme démocratique ne sera à l'abri de cette ingérence, dont les élections (celles des USA en novembre 2020 seront intéressantes à surveiller…)
- L'OTAN va poursuivre ses efforts protectionnistes : depuis 2014, si l'un de ses membres est attaqué par des moyens numériques, l'article 5 s'applique qui engage les autres membres de l'alliance
- Le plus inquiétant : l'arme numérique qui se démocratise, placée entre des mains expertes et motivées, va provoquer de graves dégâts, mais on n'a aucun moyen pour empêcher sa dissémination : il faudrait arrêter Internet, c'est une kalachnikov numérique
- Nous entrons dans une ère où plus rien ne sera incontestable et où il subsistera toujours des soupçons de malversations, de "fake news", de manipulation des informations à l'échelle des états



Cyberguerre : entre fantasmes et réalité

16 Octobre 2020

Nos prochains rendez-vous

Vendredi 23 octobre	**: Les avancées concrètes des villes intelligentes**
Vendredi 30 octobre	**: Les algorithmes de chiffrement, ces inconnus**
Vendredi 6 novembre	**: 4G et 5G privés en local, plutôt que Wi-Fi**
Vendredi 13 novembre	**: Les certifications pour remplacer les diplômes**
Vendredi 20 novembre	**: IA et la démocratie**
Vendredi 27 novembre	**: La médecine du futur, les barrières explosent**
Vendredi 4 décembre	**: La transformation digitale, mythe ou réalité**
Vendredi 18 décembre	**: Panorama des architectures globales du TI**
Mercredi 23 décembre	**: Une journée comme les autres en… 2070**